ILMU DEMI FAEDAH INSAN

Dasar Keselamatan ICT
Versi 1.0

Universiti Sultan Zainal Abidin

www.unisza.edu.my

Dasar Keselamatan ICT
Versi 1.0

Dasar Keselamatan ICT
Versi 1.0

PUSAT TEKNOLOGI MAKLUMAT
UNIVERSITI SULTAN ZAINAL ABIDIN
KUALA TERENGGANU • 2013

Diterbitkan di Malaysia oleh / *Published in Malaysia by*
Universiti Sultan Zainal Abidin
Kampus Gong Badak
21300 Kuala Terengganu
Terengganu, MALAYSIA
Tel: 09-668 7639, Faks: 09-667 1384
Laman web: http://www.ptm.unisza.edu.my

Dicetak di Malaysia oleh / *Printed in Malaysia by*
D' Integrity Design House
17681, Tingkat Bawah, Taman Semarak
Bukit Tunggal, 21200 Kuala Terengganu
Terengganu, MALAYSIA
Tel: 09-666 6111 Faks: 09-666 7111

KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT (DKICT) UniSZA yang diluluskan oleh Lembaga Pengarah Universiti (LPU) pada 15 Oktober 2012 ini mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT universiti.

Dasar Keselamatan ICT UniSZA diwujudkan untuk menjamin kesinambungan urusan universiti dengan meminimumkan kesan insiden keselamatan ICT. Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi universiti. Dasar Keselamatan ICT UniSZA boleh dicapai dengan memastikan semua aset ICT dilindungi. Objektif utama keselamatan ICT UniSZA ialah seperti berikut:

1. Memastikan kelancaran operasi pengurusan dan pentadbiran universiti.
2. Meminimumkan kerosakan atau kemusnahan aset universiti.
3. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi.
4. Mencegah salah guna atau kecurian aset ICT universiti.

Pernyataan Dasar

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyediakan dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat komponen asas keselamatan ICT iaitu:

1. Melindungi maklumat rahsia rasmi dan maklumat rasmi universiti dari capaian tanpa kuasa yang sah.
2. Menjamin setiap maklumat adalah tepat dan sempurna.
3. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna.
4. Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Dasar Keselamatan ICT UniSZA merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

1. Kerahsiaan - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.
2. Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan.
3. Tidak boleh disangkal - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal.
4. Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya.
5. Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain dari itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul, dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

Skop

Aset ICT universiti terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. DKICT UniSZA menetapkan keperluan-keperluan asas berikut:

1. Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti.
2. Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan universiti, perkhidmatan dan masyarakat.

Bagi menentukan aset ICT universiti terjamin keselamatannya sepanjang masa, DKICT UniSZA ini merangkumi perlindungan semua bentuk maklumat universiti yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

1. Perkakasan
   Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan universiti. Contohnya seperti komputer, pelayan, peralatan komunikasi dan sebagainya.

2. Perisian
   Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem adalah seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada universiti.
3. Perkhidmatan
   Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh:
   a. Perkhidmatan rangkaian seperti LAN, VPN, WAN dan lain-lain.
   b. Sistem kawalan akses seperti sistem kad akses.
   c. Sistem Pemantauan Keselamatan Kamera Litar Tertutup (CCTV).
   d. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.
4. Data atau Maklumat
   Koleksi fakta dalam bentuk kertas atau mesej elektronik yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif universiti. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod universiti, profil-profil pelajar dan staf, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain.
5. Manusia
   Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian mereka bagi mencapai misi dan objektif universiti. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.
6. Premis komputer dan komunikasi
   Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (1) – (5) di atas.

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai pelanggaran langkah-langkah keselamatan.

Prinsip-prinsip

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT UniSZA dan perlu dipatuhi adalah seperti berikut:

1. Akses atas dasar perlu mengetahui
   Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar 'perlu mengetahui' sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15.
2. Hak akses minimum
   Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna atau bidang tugas.
3. Akauntabiliti
   Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka. Akauntabiliti atau tanggungjawab pengguna termasuklah:
   a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan.

b. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa.
c. Menentukan maklumat sedia untuk digunakan.
d. Menjaga kerahsiaan kata laluan.
e. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan.
f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan.
g. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

4. Pengasingan
   Tugas mewujud, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.
5. Pengauditan
   Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*.
6. Pematuhan
   Dasar Keselamatan ICT UniSZA hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.
7. Pemulihan
   Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian

akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana atau kesinambungan perkhidmatan.

8. Saling bergantungan
   Setiap prinsip di atas adalah saling melengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

Penilaian Risiko Keselamatan ICT

Universiti hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu universiti perlu mengambil langkah -langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

Universiti hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat universiti termasuklah aplikasi, perisian, pelayan, rangkaian dan proses serta prosedur yang dikendalikan oleh universiti. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

Universiti bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

Universiti perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

1. Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian.
2. Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan universiti.
3. Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko.
4. Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

BIDANG 01

Pembangunan dan Penyelenggaraan Dasar

0101 Dasar Keselamatan ICT	
Objektif Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan universiti dan perundangan yang berkaitan.	
010101 Pelaksanaan Dasar Pelaksanaan dasar ini akan dijalankan oleh Naib Canselor UniSZA selaku Pengerusi Jawatankuasa Pemandu ICT (JPICT) UniSZA.	Naib Canselor UniSZA
010102 Penyebaran Dasar Dasar ini perlu disebarkan kepada semua pengguna universiti (termasuk pelajar, kakitangan, pembekal, pakar runding dan lain-lain).	ICTSO
010103 Penyelenggaraan Dasar Dasar Keselamatan ICT UniSZA adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT UniSZA: 1. Jawatankuasa Keselamatan ICT (JKICT)	ICTSO dan JKICT

perlu mengenal pasti dan tentukan perubahan yang diperlukan. 2. JKICT perlu mengemukakan cadangan pindaan kepada JPICT atau Mesyuarat Pengurusan Tertinggi Universiti. 3. Memaklumkan perubahan kepada semua pengguna universiti. 4. Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	
010104 Pengecualian Dasar Dasar Keselamatan ICT UniSZA adalah terpakai kepada semua pengguna ICT universiti dan tiada pengecualian diberikan.	Semua

BIDANG 02

Organisasi Keselamatan

0201 Infrastruktur Organisasi Dalaman	
Objektif Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT UniSZA.	
020101 Ketua Pegawai Maklumat (CIO) Ketua Pegawai Maklumat (CIO) bagi universiti ialah Naib Canselor (NC) UniSZA. Peranan dan tanggungjawab CIO adalah seperti berikut: 1. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT UniSZA. 2. Memastikan semua pengguna mematuhi Dasar Keselamatan ICT UniSZA. 3. Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi. 4. Memastikan penilaian risiko dan program kesedaran keselamatan ICT dilaksanakan seperti yang ditetapkan dalam Dasar Keselamatan ICT UniSZA. 5. Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JPICT), UniSZA. 6. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT universiti.	Naib Canselor UniSZA

020102 Pegawai Keselamatan ICT (ICTSO) Pegawai Keselamatan ICT (ICTSO) bagi UniSZA ialah Ketua Bahagian Keselamatan dan Audit, Pusat Teknologi Maklumat, UniSZA. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: 1. Merancang dan mengurus keseluruhan program keselamatan ICT UniSZA. 2. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT UniSZA kepada semua pengguna. 3. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT UniSZA. 4. Menguatkuasakan pelaksanaan Dasar Keselamatan ICT UniSZA. 5. Melaksanakan pengurusan risiko dalam skop keselamatan ICT universiti. 6. Melaksanakan audit, kajian semula, merumus tindak balas pengurusan universiti berdasarkan hasil penemuan dan menyediakan laporan mengenainya. 7. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian. 8. Melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan (GCERT), dan memaklumkannya kepada CIO. 9. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera. 10. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT. 11. Melaksanakan penilaian untuk memastikan tahap keselamatan ICT dan mengambil	ICTSO

tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	
020103 Pengurus ICT Pengurus ICT bagi universiti ialah ketua -ketua bahagian di Pusat Teknologi Maklumat. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: 1. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan universiti. 2. Menentukan kawalan akses pengguna terhadap aset ICT universiti. 3. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO, 4. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT universiti.	Pengurus ICT
020104 Pentadbir ICT Pentadbir ICT bagi universiti ialah kakitangan berkaitan di Pusat Teknologi Maklumat. Peranan dan tanggungjawab Pentadbir ICT adalah seperti berikut: 1. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas. 2. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan dalam Dasar Keselamatan ICT UniSZA. 3. Memantau aktiviti capaian harian sistem aplikasi pengguna. 4. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta. 5. Menganalisis dan menyimpan rekod jejak	Pentadbir ICT

audit. 6. Menyediakan laporan mengenai aktiviti capaian secara berkala. 7. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer, komputer riba, pencetak, pengimbas dan sebagainya berfungsi dengan baik.	
020105 Pengguna Pengguna adalah termasuk kakitangan, pelajar dan pihak ketiga. Pengguna mempunyai peranan dan tanggungjawab seperti berikut: 1. Membaca, memahami dan mematuhi Dasar Keselamatan ICT UniSZA. 2. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya. 3. Melaksanakan prinsip-prinsip Dasar Keselamatan ICT UniSZA dan menjaga kerahsiaan maklumat universiti. 4. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera. 5. Menghadiri program-program kesedaran mengenai keselamatan ICT. 6. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT UniSZA sebagaimana Lampiran 1. Pelajar adalah dikecualikan.	Pengguna
020106 Jawatankuasa Keselamatan ICT UniSZA Jawatankuasa Keselamatan ICT (JKICT) UniSZA adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT universiti. Keanggotaan JKICT UniSZA adalah seperti berikut: 1. Penaung Ketua Pegawai Maklumat (CIO) 2. Pengerusi Pengarah Pusat Teknologi Maklumat	JKICT UniSZA

3. Ahli: a. Timbalan-timbalan Pengarah PTM b. ICTSO UniSZA c. Pengurus ICT d. Pentadbir ICT Bidang kuasa 1. Menyediakan dokumen Dasar Keselamatan ICT UniSZA. 2. Memantau tahap pematuhan keselamatan ICT. 3. Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam universiti yang mematuhi keperluan Dasar Keselamatan ICT UniSZA. 4. Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT. 5. Memastikan Dasar Keselamatan ICT UniSZA selaras dengan dasar-dasar ICT kerajaan. 6. Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa. 7. Membincang tindakan yang melibatkan pelanggaran Dasar Keselamatan ICT UniSZA. 8. Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	
0202 Pihak Ketiga	
Objektif Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (pembekal, pakar runding dan lain-lain).	
020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: 1. Membaca, memahami dan mematuhi Dasar Keselamatan ICT UniSZA. 2. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta	CIO, ICTSO, Pengurus ICT, Pentadbir ICT dan Pihak Ketiga

melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian. 3. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga. 4. Akses kepada aset ICT universiti perlu berlandaskan kepada perjanjian kontrak. 5. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan dalam perjanjian yang dimeterai. a. Dasar Keselamatan ICT UniSZA b. Tapisan Keselamatan c. Perakuan Akta Rahsia Rasmi 1972 d. Hak Harta Intelek 6. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT UniSZA sebagaimana Lampiran 2.	

BIDANG 03

Pengurusan Aset

0301 Akauntabiliti Aset	
Objektif Memberi dan meyokong perlindungan yang bersesuaian ke atas semua aset ICT universiti.	
030101 Inventori Aset ICT Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini. b. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja. c. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di universiti. d. Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, di dokumen dan dilaksanakan. e. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pentadbir ICT, Pegawai Aset dan semua

0302 Pengelasan dan Pengendalian Maklumat	
Objektif Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
030201 Pengelasan Maklumat Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mesti mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan dalam dokumen Arahan Keselamatan seperti berikut: 1. Rahsia besar 2. Rahsia 3. Sulit 4. Terhad	Semua
030202 Pengendalian Maklumat Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: 1. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan. 2. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa. 3. Menentukan maklumat sedia untuk digunakan. 4. Menjaga kerahsiaan kata laluan. 5. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan. 6. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan. 7. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Semua

BIDANG 04

Keselamatan Sumber Manusia

0401 Keselamatan Sumber Manusia dalam Tugasan Harian	
Objektif Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan universiti, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga universiti hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.	
040101 Sebelum Perkhidmatan Perkara-perkara yang mesti dipatuhi termasuk yang berikut: 1. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan universiti serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan. 2. Menjalankan tapisan keselamatan untuk pegawai dan kakitangan universiti serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan. 3. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan.	Semua

040102 Dalam Perkhidmatan Perkara-perkara yang perlu dipatuhi termasuk yang berikut: 1. Memastikan pegawai dan kakitangan universiti serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh universiti. 2. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT universiti secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa. 3. Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan universiti serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh universiti. 4. Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Latihan dan Teknologi, PTM UniSZA.	Semua
040103 Bertukar atau Tamat Perkhidmatan Perkara-perkara yang perlu dipatuhi termasuk yang berikut: 1. Memastikan semua aset ICT dikembalikan kepada universiti mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan. 2. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh universiti dan/atau terma perkhidmatan.	Semua

BIDANG 05

Keselamatan Fizikal dan Persekitaran

0501 Keselamatan Kawasan	
Objektif Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.	
050101 Kawalan Kawasan Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat universiti. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: 1. Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko. 2. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat. 3. Memasang alat penggera atau Sistem Pemantauan Kamera Litar Tertutup. 4. Menghadkan jalan keluar masuk. 5. Mengadakan kaunter kawalan. 6. Menyediakan tempat atau bilik khas untuk pelawat-pelawat.	Pengarah Jabatan Keselamatan, Pengarah PTM

7. Mewujudkan perkhidmatan kawalan keselamatan. 8. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini. 9. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan. 10. Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana. 11. Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad. 12. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
050102 Kawalan Masuk Fizikal Perkara-perkara yang perlu dipatuhi termasuk yang berikut: 1. Setiap pengguna universiti hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas. 2. Semua pas keselamatan hendaklah diserahkan balik kepada universiti apabila pengguna berhenti atau bersara. 3. Setiap pelawat hendaklah mendapatkan pas keselamatan pelawat di pintu kawalan utama di setiap kampus. Pas ini hendaklah dikembalikan semula selepas tamat lawatan. 4. Kehilangan pas mestilah dilaporkan dengan segera.	Semua
050103 Kawasan Larangan Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di universiti adalah kawasan yang diklasifikasikan kritikal seperti bilik-bilik pegawai di	Pengurus ICT dan Pentadbir ICT

Pusat Teknologi Maklumat, Pusat Data (*Data Centre*), bilik operasi pelayan, bilik operasi rangkaian dan lain-lain. 1. Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja. 2. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	
0502 Keselamatan Peralatan	
Objektif Melindungi peralatan ICT universiti dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
050201 Peralatan ICT Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna. 2. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan. 3. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan. 4. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir ICT. 5. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya. 6. Pengguna mesti memastikan perisian antivirus	Semua

di komputer peribadi mereka sentiasa aktif dan dikemas kini secara automatik di samping melakukan imbasan ke atas media storan yang digunakan. 7. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan. 8. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran. 9. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS). 10. Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci. 11. Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai. 12. Peralatan ICT yang hendak dibawa keluar dari premis universiti, perlulah mendapat kelulusan Pengurus ICT atau Pentadbir ICT dan direkodkan bagi tujuan pemantauan. 13. Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset PTM dengan segera. 14. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa. 15. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir ICT. 16. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir ICT untuk di baik pulih. 17. Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik.	

18. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal kecuali dengan kelulusan Pengarah PTM. 19. Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan oleh Pentadbir ICT. 20. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja. 21. Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan *"OFF"* apabila meninggalkan pejabat. 22. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO.	
050202 Media Storan Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti cakera padat, pita magnetik, *optical disk*, *flash disk*, *thumb drive* dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat. 2. Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja. 3. Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan. 4. Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan,	Semua

api, air dan medan magnet. 5. Akses dan pergerakan media storan hendaklah direkodkan. 6. Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal. 7. Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data. 8. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat. 9. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
050203 Media Perisian dan Aplikasi Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan universiti. 2. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengarah PTM. 3. Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada cakera padat, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak. 4. *Source code* sesuatu sistem hendaklah disimpan dengan sistematik dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Semua
050204 Penyelenggaraan Perkakasan Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar.	Pegawai Aset PTM, Pengurus ICT dan Pentadbir ICT

2. Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja. 3. Bertanggungjawab terhadap setiap perkakasan yang diselenggara sama ada dalam tempoh jaminan atau telah tamat tempoh jaminan. 4. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan. 5. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan. 6. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.	
050205 Peralatan di Luar Premis Perkakasan yang dibawa keluar dari premis universiti adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Peralatan perlu dilindungi dan dikawal sepanjang masa. 2. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua
050206 Pelupusan Perkakasan Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekal dan ditempatkan di Universiti. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan Pusat Teknologi Maklumat, UniSZA. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran. 2. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan.	Semua, Pegawai Aset PTM, Pengurus ICT dan Pentadbir ICT

3. Peralatan ICT yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat. 4. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya. 5. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut. 6. Pegawai Aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam *Fixed Asset Management System* (FAMS) di Jabatan Bendahari. 7. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa. 8. Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: a. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman seperti RAM, *hardisk*, *motherboard* dan sebagainya. b. Menyimpan dan memindahkan perkakasan luaran seperti *IP Phone*, *speaker*, *lens* dan mana-mana peralatan yang berkaitan ke mana-mana tempat di universiti. c. Memindah keluar dari universiti mana-mana peralatan ICT yang hendak dilupuskan. d. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab PTM UniSZA. e. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit	

dan rahsia di dalam komputer disalin pada media storan kedua seperti *external drive atau thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
0503 Keselamatan Persekitaran	
Objektif Melindungi aset ICT universiti dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
050301 Kawalan Persekitaran Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai dan pembelian hendaklah dirujuk terlebih dahulu kepada Pusat Teknologi Maklumat, Jabatan Keselamatan UniSZA dan Jabatan Pembangunan dan Pengurusan Kampus. Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: 1. Merancang dan menyediakan pelan keseluruhan susun atur ruang ICT (bilik percetakan, peralatan komputer, bilik pendawaian ICT berpusat, ruang atur pejabat dan sebagainya) dengan teliti. 2. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan. 3. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan. 4. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT. 5. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT.	Semua

6. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer. 7. Akses kepada saluran *riser* hendaklah sentiasa dikunci. 8. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya sekali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	
050302 Bekalan Kuasa Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT. 2. Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan. 3. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Pengarah JPPK dan Pengarah PTM
050303 Kabel Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: 1. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan. 2. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan. 3. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping.* 4. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan	Pengurus ICT dan ICTSO

keselamatan kabel daripada kerosakan dan pintasan maklumat.	
050304 Prosedur Kecemasan Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Manual Keselamatan dan Kesihatan Pekerjaan UniSZA. 2. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Ahli Jawatankuasa Keselamatan dan Kesihatan Pekerjaan (JKKP) yang telah dilantik mengikut PTj.	Semua dan Ahli JKKP PTj
0504 Keselamatan Dokumen	
Objektif Melindungi maklumat universiti dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
050401 Dokumen Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar. 2. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan. 3. Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan. 4. Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib	Semua

	Negara. 5. Menggunakan enkripsi (*encryption*) ke atas dokumen terperingkat yang disediakan dan dihantar secara elektronik.	

BIDANG 06

Pengurusan Operasi dan Komunikasi

0601 Pengurusan Prosedur Operasi	
Objektif Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.	
060101 Pengendalian Prosedur Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal. 2. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti. 3. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua
060102 Kawalan Perubahan Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Semua

1. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu. 2. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan. 3. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan. 4. Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
060103 Pengasingan Tugas dan Tanggungjawab Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT. 2. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. 3. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Pengurus ICT dan Pentadbir ICTSO

0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	
Objektif Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
060201 Perkhidmatan Penyampaian Perkara-perkara yang mesti dipatuhi adalah seperti berikut: 1. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga. 2. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa. 3. Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua
0603 Perancangan dan Penerimaan Sistem	
Objektif Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
060301 Perancangan Kapasiti 1. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. 2. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada	Pengurus ICT dan ICTSO

perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	
060302 Penerimaan Sistem Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pengurus ICT dan ICTSO
0604 Perisian Berbahaya	
Objektif Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *trojan, malware* dan sebagainya.	
060401 Perlindungan dari Perisian Berbahaya Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat. 2. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa. 3. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya. 4. Mengemas kini anti virus dengan *pattern* anti virus yang terkini. 5. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat. 6. Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya. 7. Memasukkan klausa tanggungan di dalam	Semua

kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi perisian berbahaya. 8. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan. 9. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
060402 Perlindungan dari Mobile Code Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua
0605 Housekeeping	
Objektif Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	
060501 Backup Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu perkara yang perlu dipatuhi adalah seperti berikut: 1. Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru. 2. Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat. 3. Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan. 4. Menyimpan sekurang-kurangnya tiga generasi	Pengurus ICT, Pentadbir ICT dan semua

backup. 5. Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	
0606 Pengurusan Rangkaian	
Objektif Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
060601 Kawalan Infrastruktur Rangkaian Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan. 2. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk. 3. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja. 4. Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) sebelum pemasangan dan konfigurasi. 5. Semua pemasangan peralatan mestilah melalui proses *User Acceptance Test (UAT)*. 6. *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pengurus atau Pentadbir ICT. 7. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan PTM. 8. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna. 9. Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat universiti.	Unit Rangkaian PTM

10. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang. 11. Sebarang penyambungan rangkaian yang bukan di bawah kawalan PTM adalah tidak dibenarkan. 12. Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan.	
0607 Pengurusan Media	
Objektif Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
060701 Penghantaran dan Pemindahan Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	Semua
060702 Prosedur Pengendalian Media Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: 1. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat. 2. Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja. 3. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja. 4. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan. 5. Menyimpan semua media di tempat yang selamat. 6. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	Semua

060703 Keselamatan Sistem Dokumentasi Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: 1. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan. 2. Menyedia dan memantapkan keselamatan sistem dokumentasi. 3. Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	Semua
0608 Pengurusan Pertukaran Maklumat	
Objektif Memastikan keselamatan pertukaran maklumat dan perisian antara universiti dan agensi luar terjamin. Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
060801 Pertukaran Maklumat Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi. 2. Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara universiti dengan agensi luar. 3. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari universiti. 4. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua
060802 Pengurusan Mel Elektronik (E-mel) Penggunaan e-mel di universiti hendaklah dipantau secara berterusan oleh Pengurus ICT dan Pentadbir ICT untuk memenuhi keperluan etika penggunaan e-mel dan internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran	Semua

Awam Bilangan 1 Tahun 2003 bertajuk *Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi - agensi Kerajaan* dan mana-mana undang undang bertulis yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut:

1. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh universiti sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang.
2. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh universiti.
3. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan.
4. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul.
5. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi lima megabait (5MB) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan.
6. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui.
7. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel.
8. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan.
9. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan.
10. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat.
11. Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan

mengambil tindakan segera; 12. Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com dan sebagainya) tidak boleh digunakan untuk tujuan rasmi. 13. Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan peti mel masing-masing. 14. Pengguna adalah dilarang daripada menyebarkan *Spam* dan *junk mail*.	
0609 Perkhidmatan E-Dagang (Electronic Commerce Services)	
Objektif Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.	
060901 E-Dagang Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempromosikan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan internet. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan. 2. Maklumat yang terlibat dalam transaksi dalam talian (*online*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan. 3. Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Semua

060902 Maklumat Umum Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: 1. Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian. 2. Memastikan sistem yang boleh diakses oleh pengguna diuji terlebih dahulu. 3. Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	Semua
0610 Pemantauan	
Objektif Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
061001 Pengauditan dan Forensik ICT ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: 1. Sebarang percubaan pencerobohan kepada sistem ICT universiti . 2. Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*). 3. Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak. 4. Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan. 5. Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan. 6. Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian. 7. Aktiviti penyalahgunaan akaun e-mel. 8. Aktiviti penukaran alamat IP (*IP address*) selain	Pengurus ICT, Pentadbir ICT, ICTSO

daripada yang telah diperuntukkan tanpa kebenaran Pengurus dan Pentadbir ICT.	
061002 Jejak Audit Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: 1. Rekod setiap aktiviti transaksi. 2. Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan. 3. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya. 4. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Pentadbir ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu ke ICTSO. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	Pengurus ICT dan Pentadbir ICT
061003 Sistem Log Pentadbir ICT hendaklah melaksanakan perkara-perkara berikut: 1. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna. 2. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera. 3. Sekiranya wujud aktiviti-aktiviti lain yang tidak	Pentadbir ICT

sah seperti kecurian maklumat dan pencerobohan, Pentadbir ICT hendaklah melaporkan kepada ICTSO.	
061004 Pemantauan Log Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian. 2. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala. 3. Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan. 4. Aktiviti pentadbiran dan pengurusan sistem perlu direkodkan. 5. Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya. 6. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam universiti atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	Pengurus ICT dan Pentadbir ICT

BIDANG 07

Kawalan Capaian

0701 Dasar Kawalan Capaian	
Objektif Mengawal capaian ke atas maklumat.	
070101 Keperluan Kawalan Capaian Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna. 2. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran. 3. Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih. 4. Kawalan ke atas kemudahan pemprosesan maklumat.	Pengurus ICT , Pentadbir ICT dan ICTSO

0702 Pengurusan Capaian Pengguna	
Objektif Mengawal capaian pengguna ke atas aset ICT universiti.	
070201 Akaun Pengguna Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: 1. Akaun yang diperuntukkan oleh universiti sahaja boleh digunakan. 2. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna. 3. Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu. 4. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan universiti. Akaun boleh ditari k balik jika penggunaannya melanggar peraturan. 5. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang. 6. Pentadbir ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: a. Bertukar ke agensi lain. b. Bersara. c. Ditamatkan perkhidmatan.	Semua dan Pentadbir ICT
070202 Hak Capaian Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pengurus ICT, Pentadbir ICT
070203 Pengurusan Kata Laluan Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh universiti seperti berikut: 1. Dalam apa jua keadaan dan sebab, kata laluan	Semua dan Pentadbir ICT

hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun. 2. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi. 3. Panjang kata laluan mestilah sekurang-kurangnya 12 aksara dengan gabungan aksara, angka dan aksara khusus. 4. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun. 5. Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama. 6. Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program. 7. Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula. 8. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna. 9. Tentukan had masa pengesahan selama dua minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan. 10. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian. 11. Mengelakkan penggunaan semula kata laluan yang baru digunakan.	
070204 Clear Desk dan Clear Screen Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan	

komputer. 2. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci. 3. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	
0703 Kawalan Capaian Rangkaian	
Objektif Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
070301 Capaian Rangkaian Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: 1. Menempatkan atau memasang peralatan keselamatan yang bersesuaian antara rangkaian universiti, rangkaian agensi lain dan rangkaian awam. 2. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya. 3. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pengurus ICT, Pentadbir ICT dan ICTSO
070302 Capaian Internet Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Penggunaan internet di universiti hendaklah dipantau secara berterusan oleh Pentadbir ICT bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian universiti. 2. Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses internet. 3. Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi	Pentadbir Rangkaian Pengurus ICT Semua

menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan.

4. Penggunaan internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan internet atau sebaliknya.
5. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Pusat Tanggungjawab (PTj) / pegawai yang diberi kuasa.
6. Bahan yang diperoleh dari internet hendaklah ditentukan ketepatan dan kesahihannya. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua PTj sebelum dimuat naik ke internet.
7. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara.
8. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh universiti.
9. Penggunaan peralatan untuk tujuan sambungan rangkaian tanpa kebenaran PTM adalah dilarang sama sekali.
10. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:
    a. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti web TV, permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet.
    b. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.

0704 Kawalan Capaian Sistem Pengoperasian	
Objektif Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
070401 Capaian Sistem Pengoperasian Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: 1. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan. 2. Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: 1. Mengesahkan pengguna yang dibenarkan. 2. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user.* Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin. 2. Mewujudkan satu pengenalan diri (ID) yang unik bagi pengguna berkenaan sahaja. 3. Menghadkan dan mengawal penggunaan perisian. 4. Menghalang atau menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi dengan kelulusan Pengarah PTM.	Pengurus ICT, Pentadbir ICT dan ICTSO
070402 Kad Pintar Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Penggunaan kad pintar universiti hendaklah digunakan bagi capaian sistem - sistem yang dikhususkan.	

2. Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain. 3. Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada Pengurus ICT atau Pentadbir ICT yang berkenaan.	
0705 Kawalan Capaian Aplikasi dan Maklumat	
Objektif Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi	
070501 Capaian Aplikasi dan Maklumat Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: 1. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan. 2. Aktiviti capaian sistem maklumat dan aplikasi pengguna yang kritikal hendaklah direkodkan. 3. Menghadkan capaian sistem dan aplikasi kepada tiga kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat. 4. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah. 5. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	Pentadbir ICT dan ICTSO

0706 Peralatan Mudah Alih dan Kerja Jarak Jauh	
Objektif Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh	
070601 Peralatan Mudah Alih Perkara yang perlu dipatuhi adalah seperti berikut: 1. Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua
070602 Kerja Jarak Jauh Perkara yang perlu dipatuhi adalah seperti berikut: 1. Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua

BIDANG 08

Perolehan, Pembangunan dan Penyelenggaraan Sistem

0801 Keselamatan dalam Membangunkan Sistem dan Aplikasi	
Objektif Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.	
080101 Keperluan Keselamatan Sistem Maklumat Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat. 2. Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat. 3. Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan	Pemilik, Pengurus ICT, Pentadbir ICT dan ICTSO

sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan. 4. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	
080102 Pengesahan Data Input dan Output Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Data *input* bagi aplikasi perlu disahkan oleh pengguna bagi memastikan data yang dimasukkan betul dan bersesuaian. 2. Data *output* daripada aplikasi perlu disahkan oleh pengguna bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem dan Pentadbir ICT
0802 Kawalan Kriptografi	
Objektif Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
080201 Enkripsi Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua
080202 Pengurusan Infrastruktur Kunci Awam (PKI) Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua
0803 Keselamatan Fail Sistem	
Objektif Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	

080301 Kawalan Fail Sistem Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pengurus ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan. 2. Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji. 3. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian. 4. Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal. 5. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pemilik Sistem, Pengurus ICT dan Pentadbir ICT
0804 Keselamatan Dalam Proses Pembangunan dan Sokongan	
Objektif Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
080401 Prosedur Kawalan Perubahan Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 1. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai. 2. Mengawal perubahan dan/atau pindaan ke atas sistem aplikasi dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja. 3. Akses kepada kod sumber (*source code)* aplikasi perlu dihadkan kepada pengguna yang diizinkan.	Pemilik Sistem, Pengurus ICT dan Pentadbir ICT

4. Menghalang sebarang peluang untuk membocorkan maklumat. 5. Aplikasi pakej perisian yang dibangunkan oleh pembekal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan universiti. PTj berkaitan perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal.	
080402 Pembangunan Perisian Secara Outsource Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem. Kod sumber (*source code)* bagi semua aplikasi dan perisian adalah menjadi hak milik universiti.	Pengurus ICT dan Pentadbir ICT
0805 Kawalan Teknikal Keterdedahan (Vulnerability)	
Objektif Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
080501 Kawalan dari Ancaman Teknikal Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: 1. Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan. 2. Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi. 3. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pengurus ICT, Pentadbir ICT

BIDANG 09

Pengurusan Pengendalian Insiden Keselamatan

0901 Mekanisme Pelaporan Insiden Keselamatan ICT	
Objektif Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.	
090101 Mekanisme Pelaporan Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar Dasar Keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera: 1. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa.	Semua

2. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian. 3. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan. 4. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar. 5. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di universiti sepertimana **Lampiran 3**. Prosedur pelaporan insiden keselamatan ICT berdasarkan: 1. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi. 2. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	

0902 Pengurusan Maklumat Insiden Keselamatan ICT	
Objektif Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada universiti. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: 1. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti. 2. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan. 3. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan. 4. Menyediakan tindakan pemulihan segera. 5. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	ICTSO

BIDANG 10

Pengurusan Kesinambungan Perkhidmatan

1001 Dasar Kesinambungan Perkhidmatan	
Objektif Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
100101 Pelan Kesinambungan Perkhidmatan Pelan Kesinambungan Perkhidmatan *(Business Continuity Management - BCM*) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh Mesyuarat Pengurusan Tertinggi atau JPICT. Perkara-perkara berikut perlu diberi perhatian: 1. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan. 2. Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses	Pengarah PTM dan ICTSO

bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT. 3. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan. 4. Mendokumentasikan proses dan prosedur yang telah dipersetujui. 5. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan. 6. Membuat *backup*. 7. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali. Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: 1. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan. 2. Senarai kakitangan universiti dan pembekal berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan kakitangan tidak dapat hadir untuk menangani insiden. 3. Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan. 4. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh. 5. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh. Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut	

bersesuaian dan memenuhi tujuan dibangunkan. Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. 1. Universiti hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	

BIDANG 11

Pematuhan

1101 Pematuhan dan Keperluan Perundangan	
Objektif Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT UniSZA.	
110101 Pematuhan Dasar Setiap pengguna hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT UniSZA dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT universiti termasuk maklumat yang disimpan di dalamnya adalah hak milik universiti. Ketua PTj yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT universiti selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber universiti.	Semua
110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal CIO, Pengarah PTM dan ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	CIO, Pengarah PTM dan ICTSO

110103 Pematuhan Keperluan Audit Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua
110104 Keperluan Perundangan Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna universiti: 1. Arahan Keselamatan 2. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan 3. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002 4. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) 5. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan 6. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam 7. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan	Semua

Komunikasi (ICT) Sektor Awam 8. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network)* di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006 9. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007 10. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007 11. Akta Rahsia Rasmi 1972 12. Akta Jenayah Komputer 1997 13. Akta Hak Cipta (Pindaan) Tahun 1997 14. Akta Komunikasi dan Multimedia 1998 15. Perintah-Perintah Am 16. Arahan Perbendaharaan 17. Arahan Teknologi Maklumat 2007 18. Standar*d Operating Procedure* (SOP) ICT UniSZA	
110105 Pelanggaran Dasar Pelanggaran Dasar Keselamatan ICT UniSZA boleh dikenakan tindakan tatatertib.	Semua

GLOSARI

Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.

CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
GCERT	*Government Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab (*hub*) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu *port* kepada

	semua *port* yang lain.
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.

Logout	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
MODEM	MOdulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer

Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

Lampiran 1 Surat Akuan Pematuhan (Kakitangan)

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT UniSZA

Nama (Huruf Besar) : .....
No. Kad Pengenalan/Passport: .....
Jawatan : .....
PTj : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT UniSZA; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tanda tangan : .....
Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

.....
(Nama Pegawai Keselamatan ICT)
b.p. Pengarah Pusat Teknologi Maklumat
Tarikh: .....

Lampiran 2 – Surat Akuan Pematuhan (Pembekal)

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT UniSZA

Nama Syarikat(Huruf Besar) : .....
No Pendaftaran Syarikat : .....
Nama Wakil : .....
No. Kad Pengenalan/Passport: .....
Nama Projek : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT UniSZA; dan

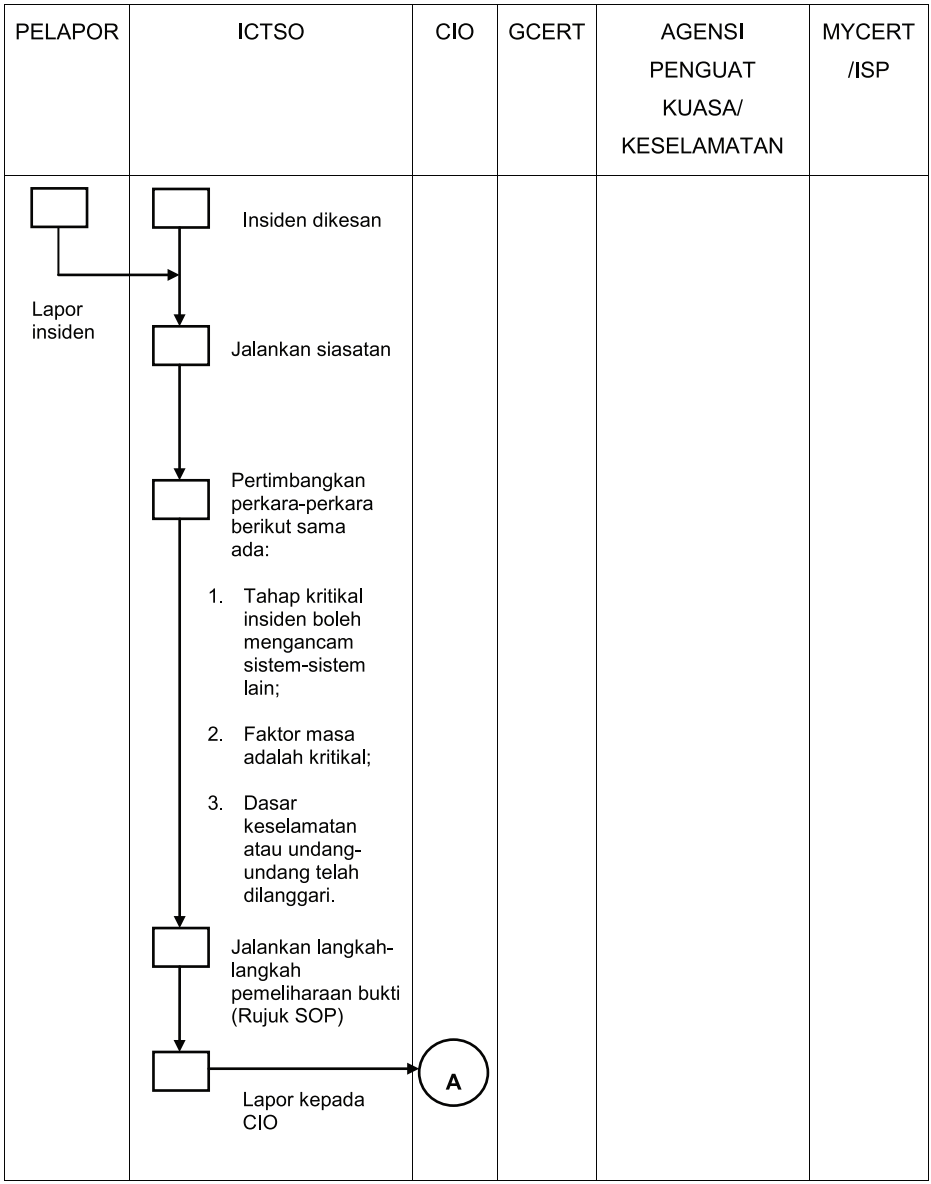
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas saya dan/atau syarikat di mana saya berkhidmat.

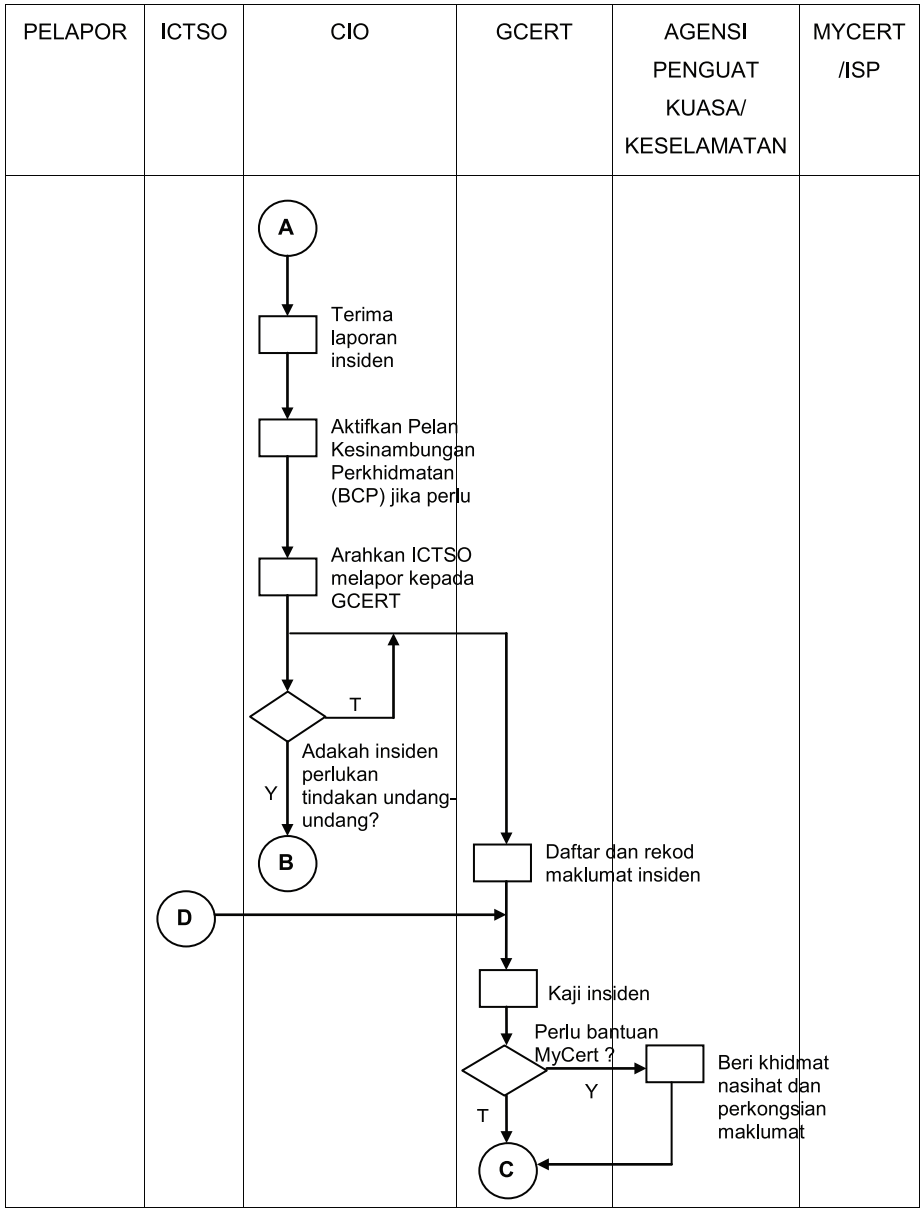
Tanda tangan : .....
Tarikh : .....
Cop Syarikat: : .....

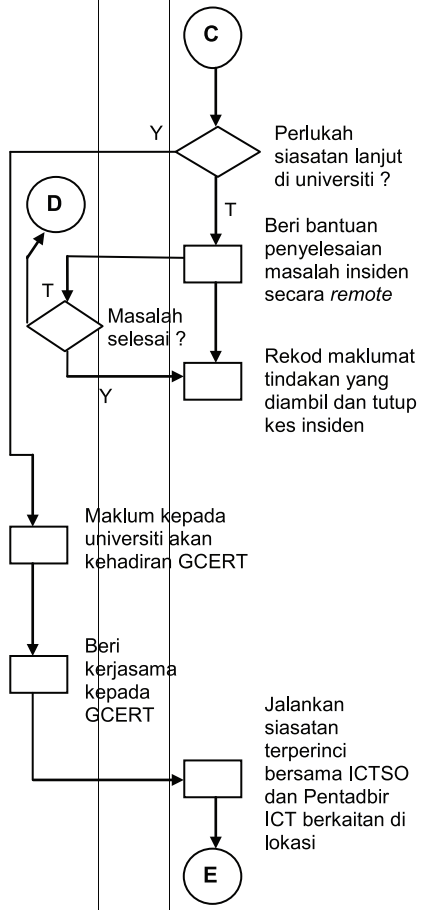
Pengesahan Pegawai Keselamatan ICT

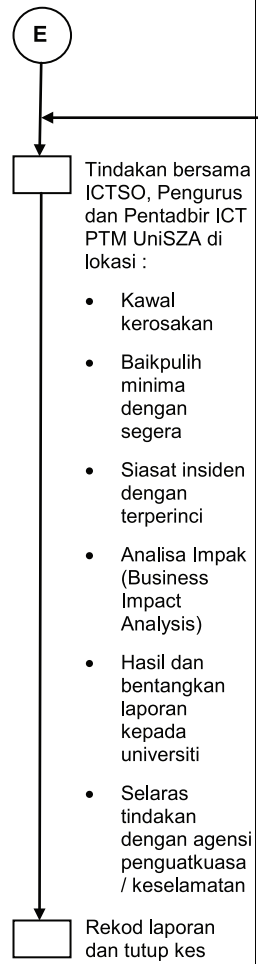
.....
(Nama Pegawai Keselamatan ICT)
b.p. Pengarah Pusat Teknologi Maklumat
Tarikh: .....

Lampiran 3 **Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT UniSZA**




PELAPOR
ICTSO
CIO
GCERT
AGENSI PENGUAT KUASA/ KESELAMATAN
MYCERT /ISP
A
Terima laporan insiden
Aktifkan Pelan Kesinambungan Perkhidmatan (BCP) jika perlu
Arahkan ICTSO melapor kepada GCERT
T
Adakah insiden perlukan tindakan undang-undang?
Y
B
D
Daftar dan rekod maklumat insiden
Kaji insiden
Perlu bantuan MyCert ?
Y
T
Beri khidmat nasihat dan perkongsian maklumat
C

PELAPOR	ICTSO	CIO	GCERT	AGENSI PENGUAT KUASA/ KESELAMATAN	MYCERT /ISP
					

PELAPOR	ICTSO	CIO	GCERT	AGENSI PENGUAT KUASA/ KESELAMATAN	MYCERT /ISP
					

يونيورسيتي سلطان زين العابدين

UNIVERSITI SULTAN ZAINAL ABIDIN

ILMU DEMI FAEDAH INSAN

Universiti Sultan Zainal Abidin
Kampus Gong Badak
21300 Kuala Terengganu
Terengganu, Malaysia

Semua pertanyaan boleh diajukan kepada:

Pusat Teknologi Maklumat
Tel: 09-668 7639 Faks: 09-668 7864
E-mel: ptm@unisza.edu.my